On Gateway Selection Protocol for DYMO-based MANET

Takeshi Matsuda*§, Hidehisa Nakayama†, Sherman Shen‡, Yoshiaki Nemoto* and Nei Kato*
* Graduate School of Information Sciences, Tohoku University,
Aramaki-Aoba 6-3-09, Aoba-ku, Sendai, 980-8579, JAPAN
† Department of Electronics and Intelligent Systems, Tohoku Institute of Technology, JAPAN
‡ Department of Electrical and Computer Engineering, University of Waterloo, CANADA
§ Phone: +81-22-795-6161, Email: george@it.ecei.tohoku.ac.jp

***Abstract*—The coupling of Mobile Ad-hoc Networks (MANETs) and the Internet is gaining attention by researchers working towards future ubiquitous computing environments. In this work, we focus on the situation that occurs when specialized, sensitive data are sent to the Internet from MANET nodes. These special data types are especially susceptible to security risks such as information leak and data falsification. Therefore, it is necessary for such special data to be forwarded by a secure/trusted gateway which is under control of a trusted network administrator. However, we assume there can be multiple gateways deployed in a MANET, where the cost ineffectiveness makes it difficult for a network administrator to simultaneously manage every gateway. Because of the risk of forwarding special data through an unmaintained gateway, we propose a routing protocol which allows a source node to have all data forwarded to the Internet through a trusted gateway. To achieve desirable performance, we improve upon one of the newest routing protocols, Dynamic MANET On-demand (DYMO). Through simulations, we evaluated our proposal in comparison with the conventional DYMO protocol. The results show that our proposal achieves performance allowing MANET source nodes to choose gateways for specific data.**

***Index Terms*—Mobile Ad-hoc Network, Routing Protocol, Mobile Internet, Security and Privacy for Ubiquitous Computing**

I. Introduction

A MANET is a collection of mobile nodes that can communicate with each other without the use of any fixed infrastructure. Every mobile node in a MANET can have the roll of both router and user, and communication is performed through multi-hop routing. In addition, the network topology can dynamically changes due to the arbitrary mobility of nodes and their ability to participate or withdraw at will.

During an event place such as concert or festival and during a disaster, it is near-impossible to communicate through any fixed infrastructure in terms of deployment cost and difficulty. However, MANETs can be deployed quite easily and efficiently, even in such temporary or emergent scenes.

Additionally, MANET is able to support connections to the Internet. If a MANET node can connect to the Internet, as well as to the other nodes in the MANET, then various advanced communication will become possible. Although connectivity to the Internet brings network scalability and bolsters ubiquitous environments, securing information becomes more challenging. In a situation such as a conference or during disaster relief, important information (medical records, business secrets, etc.) may pass through the network, in which case special attention must be paid to ensure confidentiality and data security.

Because nodes may arbitrarily participate or withdraw from a MANET at will, malicious nodes may also easily intrude. Such malicious nodes threaten a MANET's security through a wide variety of attacks (e.g. viruses, spoofing, route disruption, eavesdropping, forging or discarding data). In addition, problems can spawn from any node, for any number of reasons, including mobility issues, resource consumption, or simply from signal interference and collision. Therefore, securing the entire network by authentication mechanisms, intrusion detection systems and encryption technique is one of the most important issues.

During the coupling of a MANET and the Internet, a gateway is placed between the two networks that has direct access to both of them. It can assist with security management in the heterogeneous environment, however, we should note that such a secure gateway should be under the trusted control of a network administrator. While such gateway management can be expensive, multiple gateways or even third party access points (APs) may be deployed in a MANET along with its growth in size. This should make it quite complicated or even impossible to securely manage all the gateways and APs in a MANET.

Thus, in such an environment, the special data described above should intentionally be directed to a secure gateway. This can be achieved effectively by enabling the MANET routing protocol to allow selection of gateway depending on the sensitivity of data.

In this paper, we assume that different types of data are handled in MANET communication, multiple gateways provide Internet connectivity, and only trusted gateways may be used to forward data to the Internet. To achieve this, we propose to add additional functionality to the existing MANET routing protocol, DYMO [1]. This modification will allow DYMO to discover routes to appropriate gateways depending on the type of application data.

The remainder of this paper is organized as follows. In the next section, we first describe the coupling process between

978-0-7695-3393-3/08 $25.00 © 2008 IEEE
DOI 10.1109/WiMob.2008.51

a MANET and the Internet, and claim the significance of the routing protocols to realize such interconnection. Then we discuss the details of the DYMO protocol. Section III describes our proposed routing protocol in detail. In Section IV, the performance evaluation of the proposal is evaluated in comparison to conventional DYMO. Finally we draw a conclusion and also refer to the future works in Section V.

II. Internet Connection and the MANET Routing Protocol

Internet connectivity is an active area in MANET research and to date a significant amount of work has been conducted. One example of early work on the subject is C. Perkins's [2] proposed combination of routing by Ad hoc On-demand Distance Vector (AODV) [3] and mobility management by Mobile Internet Protocol (IP) [4]. Additionally, many architectures and systems have been recently proposed for Internet connectivity. In [5], the authors compare the operation of the most well-known approaches through logical discussions and simulations. They showed the advantages and drawbacks of those approaches. Furthermore, the influence of gateway discovery mechanisms and MANET routing protocols to the performance of those approaches was clearly specified as well. This work will greatly help to design such hybrid MANET architectures in the future. Interconnection between MANETs and the Internet brings much promise, such as the ability to extend an AP's coverage and the realization of ubiquitous computing in society.

Robust interconnection between MANETs and the Internet will require further logical and technical development in many areas including gateway and AP management, mobility management, addressing, routing, etc. As you can see from [2] and [5], routing protocols are closely related to Internet connectivity and are one of the biggest issues in this field.

While there has been much research on MANET routing protocols for Internet connectivity, research on DYMO has mostly been conducted concerning multipath routing [6] and secure routing [7]. As of yet, no research concerning Internet connectivity and MANETs while using DYMO has been conducted.

A. MANET Routing Protocols

As routing protocols are one of the main challenges in MANET, a good number of MANET routing protocols have been proposed. They are largely categorized into Reactive and Proactive schemes.

The reactive protocols such as AODV and Dynamic Source Routing (DSR) [8], enable on-demand route discovery and offer low processing, memory overhead, and network utilization. On the other hand, proactive protocols such as Optimized Link State Routing (OLSR) and Topology Dissemination Based on Reverse-Path Forwarding (TBRPF), enable every node to comprehend the entire network topology and to initiate a connection quickly according to periodic information exchange.

Currently the Working Group (WG) of the Internet Engineering Task Force (IETF) is conducting research regarding practical MANET use, including developing a unified packet format [9] and working towards a standardization of routing protocols. DYMO is one of their perspective protocols and grabs attention as the future representative of reactive routing protocols.

B. DYMO Routing

DYMO is a successor of AODV, so its routing algorithm is naturally similar to that of AODV. Nevertheless, there are many remarkable changes such as a unified packet format, a simplified RERR algorithm, and multiple interface utilization. Furthermore, the Internet connectivity is also defined in the DYMO Internet-Draft [1], and is the most attractive specification yet towards practical MANET use. Next, we will outline the core routing and Internet connection algorithms of DYMO.

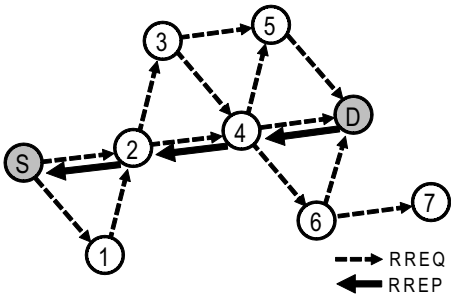
As DYMO is a type of reactive routing protocol, it consists of two operations: route discovery and route maintenance.

The route discovery begins with the flooding of Route Request (RREQ) messages by a source node. As shown in Fig. 1a, RREQ is broadcast from source S, received by the neighbor nodes of S, then re-broadcast. This multihop transmission will allow the RREQ to reach the expected destination D. In response to the RREQ, D unicasts Route Reply (RREP) messages toward S. This RREP will eventually reach the source node through the multihop path. In this way, the route from S to D is established. It should be noted that this path is the shortest path out of all possible routes, and is loop-free. The intermediate nodes which forwarded both the RREQ and RREP messages take the roll of routers. The route S–2–4–D is established in Fig. 1a.

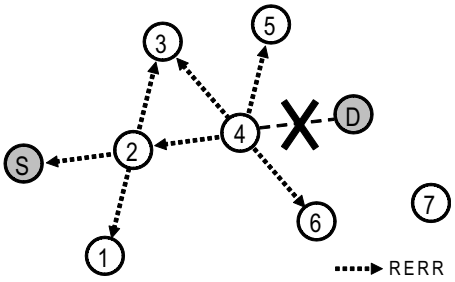
Because each node serves as a router, every node maintains its own routing table, which consists of a destination IP, next hop IP, sequence number, route timeout, and also the information if the destination is gateway or not. Multiple entries for the same destination in a routing table cannot exist. When nodes receive or successfully send a message, they update the information in the routing entry according to the message. In this way, every active route is kept fresh, loop-free and with the smallest number of hops.

When an intermediate node finds a broken link, or when it receives a datagram and does not know where to forward it, it broadcasts a Route Error (RERR) message with the information about the unreachable destination. RERR messages are forwarded by intermediate nodes until the message reaches the source node of the broken route or the no-route datagram. In Fig. 1b, node 4 discovers the link to D is broken and broadcasts a RERR. The RERR is sent to S through the intermediate node 2.

In addition to the above routing operations, Internet connectivity is also defined in the DYMO Internet-Draft. The existence of a gateway is essential to establish a connection to the Internet. The gateway is assumed to know all the MANET nodes IP addresses beforehand. When a MANET node tries to discover the route to a destination on the Internet, it broadcasts RREQ as well as the normal route discovery process described above. The gateway can then judge if the destination of the



(a) RREQ Broadcasting and RREP Unicasting



(b) RERR Broadcasting

Fig. 1. DYMO Routing Messages

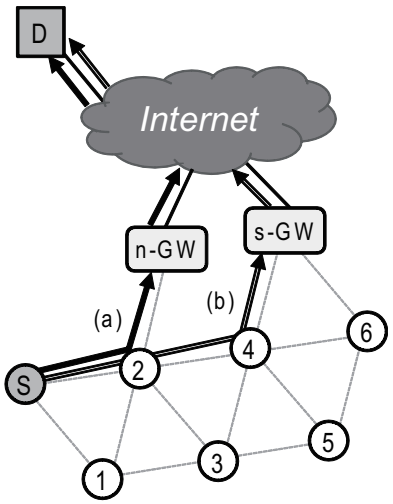


Fig. 2. Data Transmission to the Internet

received RREQ is outside the MANET. Once it has the route to the destination on the Internet, it finally initiates RREP for the source node on behalf of the true destination.

The DYMO draft also allows for multiple gateways in a MANET, which should be powerful when the size of a MANET is too large to be covered by a GW. In the topology of Fig. 2, both of the two gateways receive the RREQ from source S, and return RREP to S. As a result, S receives two different RREPs to the same destination. According to the DYMO algorithm, nodes prefer the minimal hop route, so only route (a) is used for data transmission to D.

III. Proposed Method

The DYMO Internet-Draft defines that one or more gateways are necessary for Internet connectivity. We assume that the special sensitive data are handled on these multi-gateway MANETs. Our DYMO routing algorithm directs the special data to a specific secure gateway, while conventional DYMO route discovery does not.

First, we classify application data into two types. Special-data (s-Data) which includes important, sensitive or advanced information that requires particular security considerations, and normal-data (n-Data) which has no such requirements. While n-Data can be forwarded by any gateway, s-Data must be forwarded by only special gateways (s-GW), which are operated by a trusted network administrator.

Based on these assumptions, our proposal uses two types of routes, namely routes for n-Data (n-Route) and routes for s-Data (s-Route). For this purpose, we also classify Routing Messages (RMs), gateway and routing entries according to these data types.

A. Data and Routing Message

The data type variation is reflected in the Type of Service (ToS) field in the IP header. Every node can judge the data type by its ToS field.

When a source node wants to send s-Data, it begins s-Route discovery with a special-RREQ (s-RREQ). The RREP for the s-RREQ also must be a special-RREP (s-RREP), while normal-RREP (n-RREP) is the response to the normal-RREQ (n-RREQ).

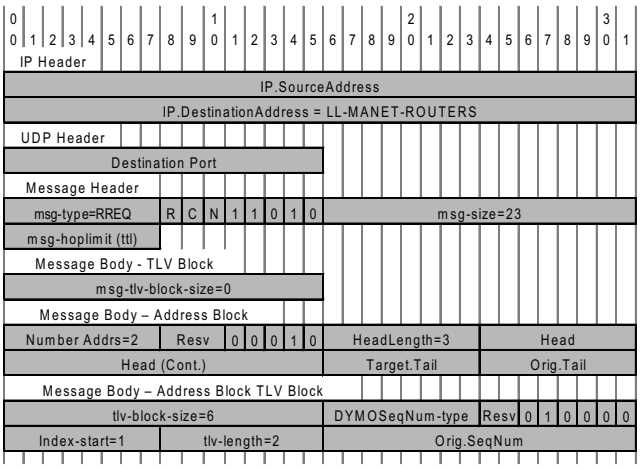
This variation of RMs is determined by the S flag in the message header. Fig. 3a shows the generic DYMO RREQ format. The 8-bit field between msg-type and msg-size is called msg-semantics, and describes the interpretation of the rest of the message header [9]. These bits express whether the message header contains a msg-version, originator address, sequence number, or hop count, etc. The most significant bit for our purposes is the R-bit, which means reserved and has no use in the entire MANET specification.

Hence, we apply this reserved bit to the S-flag as shown in Fig. 3b. When S is 0, the message is n-RREQ or n-RREP, and when S is 1, the message is s-RREQ or s-RREP. Each MANET node checks the S-bit in the received RM to recognize its type.

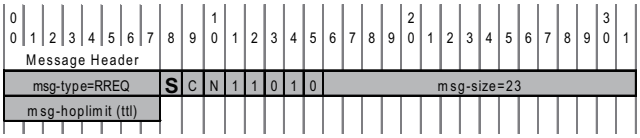
B. Gateway

We define a trusted gateway that can forward both n-Data and s-Data as special-gateway (s-GW). A gateway that is only trusted to forward n-Data is called a normal-gateway (n-GW). Fig. 4 depicts the RREQ reception algorithm which represents the difference between a n-GW and s-GW. Both types of gateways respond to n-RREQ with n-RREP. However, n-GWs do not respond to s-RREQ, therefore only s-GWs return s-RREP. In this way, the source node that sends an s-Data can limit the relaying gateways to s-GWs.

We explain how the proposed routing method affects route discovery for s-Data in Fig. 2. With our proposed routing method, the s-Data owned by S must be transmitted through



(a) DYMO RREQ Format



(b) Embedding S-flag on msg-header

Fig. 3. DYMO Packet Format and Modification

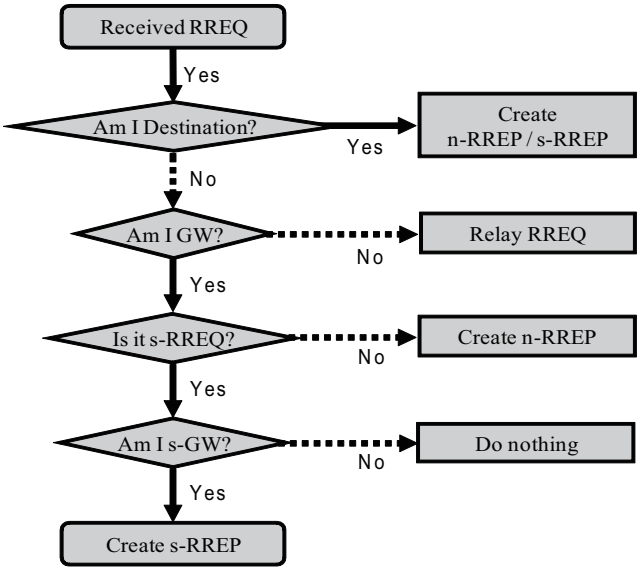


Fig. 4. Algorithm of the Response to Received RREQ

route (b), even though there is a shorter route (a) which would normally be selected by the DYMO algorithm. Thus, our proposal considers both the type of data and the gateway, as well as the hop count.

C. Routing Entry

To achieve the desired routing behavior, we must also modify the definition of routing entries by attaching S-flag. S-flag can be used to identify the type of routing entry: entries

TABLE I
EXAMPLE OF THE ROUTING TABLE OF NODE 2 IN FIG. 2

Destination	Sequence Number	Hop Count	Next Hop	S
S	...	1	S	0
S	...	1	S	1
D	...	1	n-GW	0
D	...	2	4	1
...	...	...	...	...

TABLE II
SIMULATION ENVIRONMENT

Parameter	Value
Simulation Time	10 min.
Number of Executions	100
Dimension	1800m x 1800m
Number of Nodes	MN: 91, GW: 9
Node Placement	Random (GW: fixed)
Mobility Model	Random Waypoint (GW: none)
Min. Speed	0 m/s
Max. Speed	5 m/s
Pause Time	10 sec.

TABLE III
CBR DATAGRAMS SETUP

	n-Data	s-Data
Number of Flows	5	5
Data Size	512 bytes	512 bytes
Communication Period	1-9 min.	4-6 min.
Sending Rate	2.5 packet/s	10 packet/s

with S=0 are for n-Data, while those with S=1 are for s-Data. Therefore, a MANET node can have two routing entries which have the same destination but different S value as shown in TABLE I. Traditional DYMO only allows for one entry per destination.

IV. PERFORMANCE EVALUATION

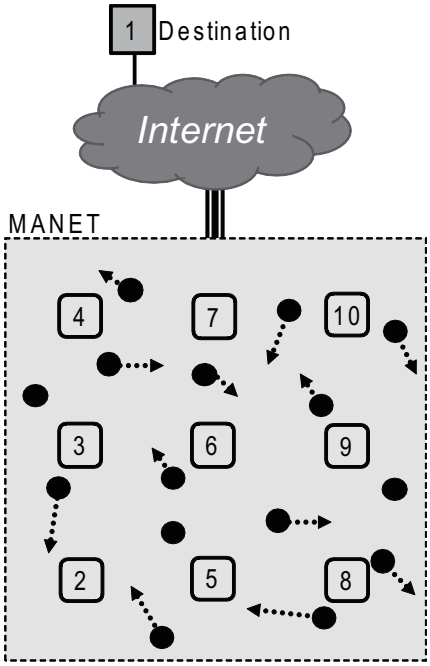
A. Simulation Setup

We used the commercial simulator QualNet 4.0 [10] to implement our proposed method by modifying DYMO which comes preinstalled. To check whether it performs the expected routing operations, we conducted different experiments.

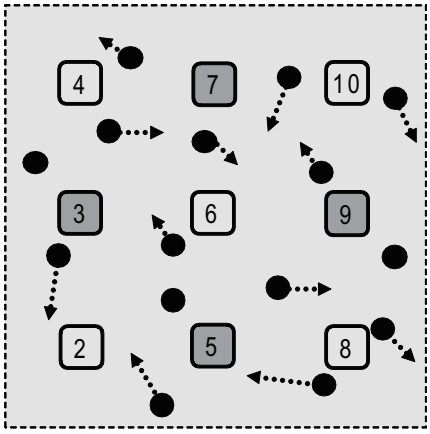
The objective in the simulated scenario is for the MANET nodes to transmit n-Data and s-Data to a fixed node on the Internet by using the MANET gateways. We use a Constant Bit Rate (CBR) for transferring n-Data and s-Data. Each experiment conducts the simulation 100 times, each with different random value seeds to accurately account for the fact that mobile nodes are located randomly. The nodes also move based on Random Waypoint Mobility Model [11]. Each of the following results are an average of 100 simulations. We also introduce other configurations in TABLE II, III.

All simulations were preformed on the topology shown in Fig. 5a. Gateway 2-10 are fixed evenly in the simulation field and every data packet should be delivered by either of them. In the simulation environment, we introduced three different experiments as follows:

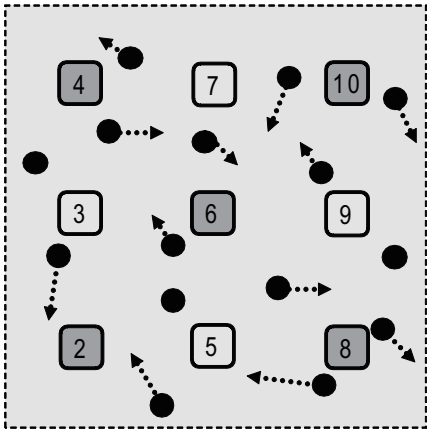
1) Exp. 1: The control simulation with conventional DYMO. The results of our proposal will be compared to this.



(a) with DYMO, 9 Gateways



(b) with Proposal (s-GW: 3, 5, 7, 9)



(c) with Proposal (s-GW: 2, 4, 6, 8, 10)

Fig. 5. Simulation Topologies

TABLE IV
TOTAL TRANSMISSION RESULT OF DATAGRAMS

	Exp. 1	Exp. 2	Exp. 3
Total Sent	12000		
Average Received	11827.80	11000.50	11161.80
Average Dropped	172.20	999.50	838.20
Delivery Ratio	98.57 %	91.67 %	93.02 %

2) Exp. 2: Used the same architecture as Exp. 1, except with applying our proposed routing protocol. Gateways 3, 5, 7, 9 are set to s-GW, while the others remain n-GW, as shown in Fig. 5b.

3) Exp. 3: This experiment is the same as Exp. 2, except the location of gateways was changed as shown in Fig. 5c: gateways 2, 4, 6, 8, 10 are s-GW, the others are n-GW. This change was made to prove that the proposed route discovery leads s-Data to an s-GW without relying on any particular location of s-GWs.

B. Simulation Results

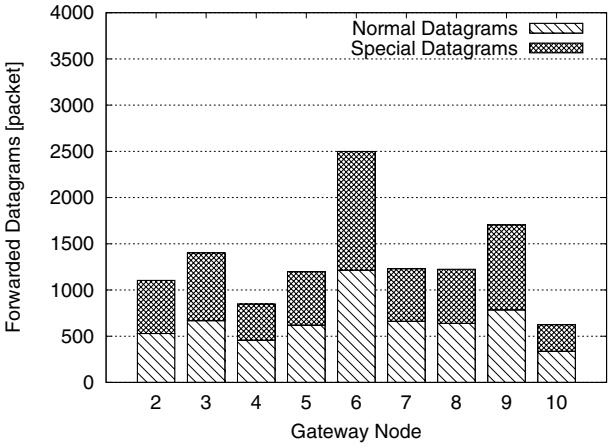
Fig. 6 depicts the average number of n-Data and s-Data forwarded by the gateways in each experiment. The result of Exp. 1 in Fig. 6a, shows that every gateway forwards datagrams without any regard for data type. On the other hand, Fig. 6b depicts the result of Exp. 2, which uses our proposed method that directs all s-Data to only s-GWs. We can also see the same behavior from the result of Exp. 3 in Fig. 6c. Like Exp. 2, only s-GWs handle s-Data. Moreover, the difference between the result of Exp. 2 and that of Exp. 3 shows that our proposal can select s-GWs wherever they are deployed.

The average packet transmission for each experiment is shown in TABLE IV. The number of drops for our proposal (Exp. 2, 3) is clearly greater than that of conventional DYMO (Exp. 1). In our proposal, because all s-Data is directed to s-GWs, a traffic imbalance occurs between n-GWs and s-GWs. As a result, s-GW and mobile nodes around the s-GW lose packets due to signal collision, interference, and queue overflow. Additionally, the number of drops in Exp. 3 is less than that of Exp. 2 because Exp. 3 has more s-GWs.

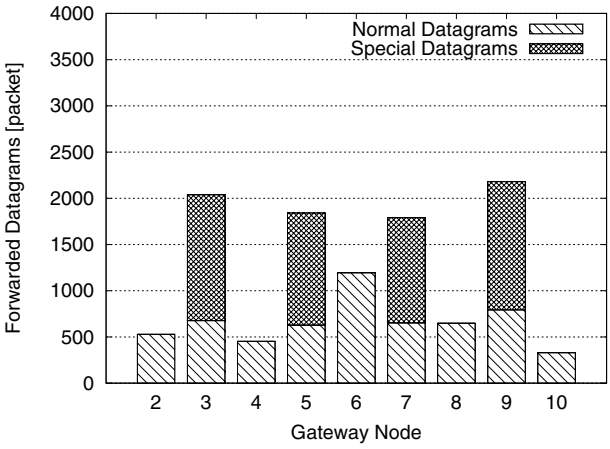
V. CONCLUSION AND FUTURE WORK

Internet connectivity for MANETs is quite attractive in terms of increased variety in communication, and network expansion and accessibility. We proposed a routing protocol which allows source nodes to forward special sensitive data to the Internet through specially secure/trusted gateways. This ensures that advanced and important data are handled securely by a gateway that is under the trusted control of a network administrator.

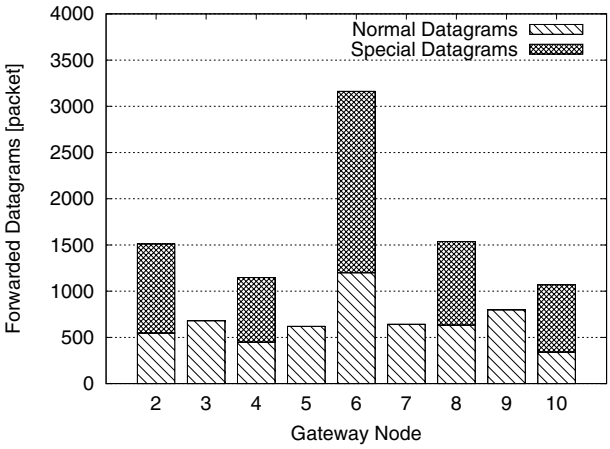
Our proposal is implemented through the modification of DYMO. Conventional DYMO is agnostic to the character of data and trustworthiness of gateways, and instead uses only hop count as a metric for the route discovery process. To include the character of data and gateways into the DYMO routing metrics, we classified data into sensitive and normal data. The RMs, gateways and routing entries are also classified



(a) with DYMO



(b) with Proposal (s-GW: 3, 5, 7, 9)



(c) with Proposal (s-GW: 2, 4, 6, 8, 10)

Fig. 6. Type and Number of Forwarded Datagrams by Gateways

according to their relevant data type so that the routes are individually established for each combination: source, destination, and data type.

Simulation results show that our proposal correctly selects the s-GW for transmission of the s-Data, however this comes at a cost of increased packet drop. To mitigate traffic concentration on s-GWs and the mobile nodes around them, implementation of an appropriate load balancing mechanism will be examined in future works.

REFERENCES

[1] I. Chakeres and C. Perkins, "Dynamic MANET on-demand (DYMO) routing," IETF Internet Draft, draft-ietf-manet-dymo-12, Feb. 2008.

[2] Y. Sun, E. M. Belding-Royer, and C. E. Perkins, "Internet connectivity for ad hoc mobile networks," *International Journal of Wireless Information Networks*, vol. 9, no. 2, pp. 75–88, Apr. 2002.

[3] C. E. Perkins, E. M. Belding-Royer, and S. R. Das, "Ad hoc on-demand distance vector (AODV) routing," RFC 3561, Jul. 2003.

[4] C. Perkins, "IP mobility support for IPv4," RFC 3344, Aug. 2002.

[5] R. P.M., R. F.J., and G.-S. A., "Internet connectivity for mobile ad hoc networks: Solutions and challenges," *IEEE Communication Magazine*, vol. 43, no. 10, pp. 118–125, Oct 2005.

[6] J. J. Galvez and P. M. Ruiz, "Design and performance evaluation of multipath extensions for the DYMO protocol," in *Proc. of the 32nd IEEE Conference on Local Computer Networks(LCN '07)*. Washington, DC, USA: IEEE Computer Society, 2007, pp. 885–892.

[7] H. Rifa-Pous and J. Herrera-Joancomarti, "Secure dynamic MANET on-demand (SEDYMO) routing protocol," in *Proc. of the Fifth Annual Conference on Communication Networks and Services Research (CNSR)*, May 2007, pp. 372–380.

[8] D. Johnson, Y. Hu, and D. Maltz, "The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4," RFC 4728, Feb 2007.

[9] T. Clausen, C. Dearlove, J. Dean, and C. Adjih, "Generalized manet packet/message format," IETF Internet Draft, draft-ietf-manet-packetbb-11, Nov. 2007.

[10] S. N. Technologies, "Qualnet," http://www.scalable-networks.com/.

[11] C. Bettstetter, G. Resta, and P. Santi, "The node distribution of the random waypoint mobility model for wireless ad hoc networks," *IEEE Trans. Mobile Computing*, vol. 2, no. 3, pp. 257–269, July–September 2003.